EXHIBIT 24

3-June-96

SW Functional Spec Rev 3.0
Author: Bill Westfield
Project Mgr: Andy Valencia

Radius Protocol Support

Abstract

RADIUS is an access server authentication and accounting protocol developed by Livingston, Inc. It has gained support amoung a wide customer base, and is expected to be run through the IETF for standardization as a NAS authentication protocol. RADIUS is currently defined in draft documents on ftp.livingston.com:pub/radius/draft-ietf-radius-radius-03.txt. The cisco implementation will be based on this version of the draft, and attempts will be made to keep up with any newer drafts issued.

Approvals

Modification History

Rev	Date	Originator	Comment
1.0	950504	Bill Westfield	Initial Release
2.0	950823		Add list of radius attributes supported Add documentation for formats of NAS dependent attribute formats. Mention features that didn't get implemented.
3.0	060603		Add info about "features" added after FCS.

1.0 Definitions

Authentication - The means by which you IDENTIFY your self to the cisco.

Authorization - The means by which the cisco determins what actions you mat perform.

Accounting - the means by which the cisco tracks what you have done.

AAA cisco's security paradigm (Authentication, Authorization, Accounting) In theory, AAA is protocol independant.

TACACS+ cisco's network protocol for implementing AAA. TACACS+ is tcp based.

NAS - Network Access Server. The cisco Access Server, or other cisco hardware, that is acting as the client fo the authentication protocol.

2.0 Problem Definition

Some large customers have settled on RADIUS as their standard for network based authentication, and request that we implement it. Radius does not appear to have any features not supported by Tacacs+, and lacks a few nicities that would allow it to map cleanly onto AAA, so it should be moderately easy to add support for.

The most important consideration are to support per-user service definition and network profiles. Eg, when user "billw" logs in, RADIUS must be able to specify that ppp using ip address x.y.z.a and access-list N should be started.

3.0 Design Considerations.

Radius combines the Authentication and Authorization functions, so the NAS will have to "remember" authorization information from the authentication response, and supply that later on when requested by authorization. The NAS must be configured for the appropriate authorization or it will ignore that data from the authentication packet.

RADIUS is UDP based. A single process should be responsible for multiplexing and demultiplexing multiple authentication "streams" between the NAS and the Radius Server. While we're at it, do this for tacacs+ as well.

RADIUS should be a separate subsystem, so that it can be omitted from images (eg rxboot) where it is inappropriate.

RADIUS accounting is not explicitly set up to deal with multiple connections during a single exec session, so the following conventions will be used:

AAA ACCOUNTING EXEC

This will result in radius accounting records with Service-type set to "Shell-User". These records will not contain any traffic statitistics, but include elapsed time and may be useful for tracking the total time a user is logged in.

AAA ACCOUNTING CONNECTION

This will result in radius accounting records with Service-type set to "Login-User", with traffic statistics for the connection when they are available (ie not for LAT.) Telnet, tcp, and tn3270 sessions will be identified with "Login-Service=telnet". LAT sessions will have "Login-Service=LAT" and "Login-LAT-Service=name". X.25 PAD connections, for lack of anything better to do, will have "Login-LAT-Service=x121address", but won't include any "Login-Service". Note that in a typical radius-controlled login session where a user gets a connection immediately upon login and is logged out when that connection is complete, exec and connection accounting will provide nearly identical start and stop times, but the connection accounting will have additional info about type, destination, and traffic.

AAA ACCOUNTING NETWORK

Will result in radius accounting packets pretty much as described in the draft specification, since the cisco model also terminates the users session when the network session ends. Note that an exec user who starts SLIP or PPP will not produce an exec stop record until the end of the network session (the network and exec sessions will overlap.)

4.0 Memory and Performance Impact.

The RADIUS code should add less than 30k to the image size, use negligible memory other than packets queued awaiting answers, and have negligible performance impact in general and none in any critical paths.

5.0 End User Interface.

No new end user interface. (Note that radius is capable of supplying login dialog to the user during authentication, and can provide a different user interface there.)

6.0 Configuration and Restrictions.

It should be possible to specify "radius" anywhere in config files where "tacacs+" is currently usable. Authentication and authorization lists that allow multiple protocols to be specified should allow both tacacs+ and Radius, in either order.

aaa authentication <feature> <listname> RADIUS

aaa authorization <feature> RADIUS

aaa accounting <feature> <when> RADIUS

In addition, a set of top level "radius-server" commands analagous to the "tacacs-server" commands will be added:

radius-server host <list> [auth-port <n>] [acct-port <n>]

> Server host to use. Multiple hosts may be configured. The implementation will try each host in the list, if the previous host fails to respond withing the retransmissions and timeout specified. auth-port, if included, specifies the UDP destination port for authentication requests. acct-port specifies the UDP port for accounting requests. If either is set to zero, this host will not be used for that type of request.

radius-server key <string>	Shared secret (Key) for encryption and server authentication.
radius-server retransmit <n>	Max number of retransmission attempts.
radius-server timeout <n>	Time between retransmisions.
radius-server deadtime <n>	If a radius server fails to respond to a request, mark it as "dead" for the next n minutes. It will then be skipped when picking a server to use for additional requests, unless there are no servers NOT marked dead.
radius-server directed-request	Allow user to specify "@server"

(not implemented)

radius-server refuse-unimplimented (not implemented)

This is new. For features that are implemented in the cisco NAS, but are not supported by the current version of the radius protocol, refuse to let the user use those features. The default is "no radius refuse", which allows the feature to be used without attempting a radius transaction.

radius-server shell-doauth (???) (not implemented)

This command is an attempt to use radius authentication calls to do authorization. If the Server grants the user "shell" access during the initial authentication, the NAS will normally allow any shell commands that are not explicitly disallowed by any additional authorization info from that original authentication. If "radius shell-doauth" is configured, the NAS will issue additional authentication requests for new commands, with no password included (this is one suggested method of doing authorization within the current radius protocol.) Few servers are expected to support this.

7.0 Testing Considerations.

Should be tested against existing radius servers from UWisc/etc.

The radius specification is a draft and subject to change. It can change faster than the radius servers we are using to test with. The list here is derived from the May, 1995 draft.

The follow radius attributes will be supported by the cisco radius implementation. In cases where the attrbute has a NAS specific format, the format is described here.

User-Name
User-Password
CHAP-Password
NAS-IP-Address
NAS-Port
numeric tty number for async lines. For non async interfaces, contains the first two bytes of the interface name in the high 16 bits, and the (first) interface unit number for the low 16 bits.
(ie, for BRI0, would contain 'B' 'R' '\0' '\0')
Service-Type
in a request:
Framed for known PPP or SLIP connections (autoselect, ISDN)
Administrative-user for enable command.
Not included for "normal" ascii login.
In response:
Login - make a connection
Framed - start slip or PPP
Administrative User - start an exec, or enable ok.
Shell User - start an exec.
Framed-Protocol

Framed-IP-Address An address of 0xFFFFFFFE will cause the IOS to select
either the default peer address configured, or an address from the
default ip pool if pools are configured.

Framed-Routing
"None" and "send and listen" supported.

Filter-Id
should have a format of %d, %d.in, or %d.out Associated with the
most recent Service-type command. For login and exec, use %d or
%d.out as the line access list value 0<n<199. For Framed service,
use %d or %d.out as interface output access list, %d.in for input
access list. The numbers are self-encoding as to which protocol
they refer to.

Framed-Compression
results in "/compress" being added to the PPP or SLIP autocommand
generated during exec authorization. Not currently implemented for
non-exec authorization.

Login-IP-Host
Login-Service
Login-Port

Reply-Message
displayed to user.

Session-Timeout
becomes per-user "absolute-timeout" for exec sessions.

Idle-Timeout
becomes per-user "session-timeout"
Callback not currently supported

Login-LAT-Service
Login-LAT-Node
Login-LAT-Group

Framed-Route
The format suggested in the specification is supported
("net/bits [router [metric]]") We also support the use of
the old style dotted mask ("net mask [router [metric]]") If
the "router" is omitted or 0, we use the peer ip address
(possibly from framed-ip-address attribute). Mertics are
currently ignored.

State is propagated from access-challenge packets into the subsequent
access-request. A user message from the accesss-challenge is
displayed to interactive login users, and the additional input
is accepted without additional prompting (this means your message
should look like a prompt!)

Vendor-Specific
The cisco radius implementation will support one vendor specific
option using the format recomened in the specification. Cisco's
"vendor-ID" is 9, and the supported option has vendor-type 1,
which is named "cisco-avpair". The value is a string of the format:

```
protocol : attribute sep value
```

"protocol" is a value of the the cisco "protocol" attribute for a
particular type of authorization. "attribute" and "value" are
an appropriate AVpair defined in the cisco tacacs+ specification,
and "sep" is "=" for mandatory attributes and "*" for optional
attributes. This allows the full set of features available for
tacacs+ authorization to be used from radius as well. Consider:

```
cisco-avpair=     "ip:addr-pool=first"
cisco-avpair=     "shell:priv-lvl=15"
```

The first example causes cisco's "multiple named ip address pools" feature to be activated during IP authorization (ie during PPP's IPCP address assignment.) The second example will cause an interactive shell user to immediately have access to "privledged" exec commands.

Class

If an Access-Accept contains a "Class" attribute, it will be included in all Accounting-Requests generated during that user's session.

The following radius attributes are not currently supported in the IOS implementation:

NAS-Identifier (uses NAS-ip-address instead)
Framed-IP-Netmask
Framed-Routing
broadcast-only and listen-only not supported
Framed-MTU
Framed-Compression
Not supported on dedicated IP links.
Login-Callback-Number
Framed-Callback-Id
Login-Callback-Number
Framed-Callback-Id
Framed-IPX-Network
Termination-Action
Called-Station-Id
Calling-Station-Id
Proxy-State
Login-LAT-Group
Framed-AppleTalk-Link
Framed-AppleTalk-Network
Framed-AppleTalk-Zone

8.0 Reference Documents.

AAA specification. TACACS+ Specification. Radius draft specification.